総務省 利用者視点を踏まえたICTサービスに係る諸問題に関する研究会
スマートフォンを経由した利用者情報の取扱いに関するWG 第3回
2012年3月8日 配布資料

資料2

情報取得手段ごとに相当な同意確認基準の提案

産業技術総合研究所
情報セキュリティ研究センター
高木 浩光

背景：ウェブからスマホアプリへ

- ウェブ
  - セキュリティ制約による厳しい機能制限
    - どのサイトを不意に訪れても問題が生じないよう機能を制限
    - 収集できるのは利用者が自発的に入力した情報に限られる（同意確認不要）
    - 端末ID的な機能（super cookie）は徹底排除されている
    - 位置情報の使用はサイト単位でオプトイン方式（ブラウザの機能2009年～）
  - 少数のブラウザベンダにより事実上の標準が確立していた
    - 結果としてコンテンツプロバイダはその上で可能なことは何でも無断でやってよい
  - しかし利便性に限界（例：Java Appletは衰退）
- スマホアプリ
  - 中間的な緩さの機能制限
    - 一般のPCのプログラムのようには自由でない（マルウェア蔓延の防止）
      - 例：他のアプリのデータを参照することはできないが、アドレス帳は読める等
    - 「iアプリ」よりは制限が緩い
      - 例：任意のサイトと通信できる、同意確認なしにアドレス帳を読める等
  - 個々のアプリ提供者の裁量 → 新しい問題が発生

Permission確認方式の限界

- PermissionはJavaの基本機能（J2SE 1.2 1998年〜）
  - ウェブ用Appletでpermissionを利用者が確認するという方式が採用されることはなかった
    - WindowsのActiveXコントロールで一時期近い方式はあったが廃止になった（利用者に見せても判断できずナンセンス）
  - Androidがそれを採用
    - ウェブと異なりインストールを要することから利用者に責任を転嫁
- 使用と送信の許可が独立
  - 例：位置情報を使用することと、何かを外部に送信することは別々のpermissionで制御される
  - 「送信しない使用」と「送信する使用」を区別できない
    - これを区別して許可するpermissionモデルは技術的に実現不可能
  - 各情報の送信に同意したことにはならない
    - 各情報の使用への同意と、何らかの情報の送受信に同意したにすぎない

同意確認のレベル

- オプトイン方式（細目に分けるべき）
  - 強制オプトイン（仮称）
    - 同意しなければ一切の利用ができない
      - 利用者は理解が足りないまま同意ボタンを押しがち
  - 包括的選択オプトイン（仮称）
    - アプリ全体に対して起動時に同意を求め、拒否しても利用ができる
      - 利用者は理解が足りないまま同意ボタンを押しがち
  - 個別的選択オプトイン（仮称）
    - アプリ使用中に当該機能を使用する段になって同意を求める
      - 利用者は状況の流れから何が起きるか理解しやすい
- オプトアウト方式（Do Not Track対応を含む）
  - ポリシーや規約に書かれ、拒絶手段が用意される
- 黙示の同意（仮称）
  - ポリシーや規約に書かれているだけで、拒絶手段なし

基本的な考え方

- 利用者の意図に反した動作とならないようにする
  - 不正指令電磁的記録に関する罪（刑法168条の2 ）との関係
  - 個人情報保護法17条 偽りその他不正な手段によらない取得
  - 当該機能の存在を利用者が予見できるか
- 歴史的経緯（国際的な）を踏まえる
  - 意図に反するか否かは、社会通念に照らしその機能につき一般に認識すべきと考えられるところを基準とする
- サービス実現のための技術的必然性があるか
  - 利用者が期待するところのサービスの実現にとって
  - 必要最小限の技術手段を用いるべき
- 取得情報の範囲が利用者の想定し得る範囲内か
- 情報元の種類による個別の判断

IDの匿名性レベル

- アプリ間で共通で使用されるID（グローバルID）
  - IMEI、UDID、MACアドレス、Android_ID等、及びそれから変換された値（ハッシュ値等）
  - 提供先や流出先で個人が特定され得る
    - 個人情報保護法23条（第三者提供の制限）の趣旨に触れる
    - 個人情報保護法20条（安全管理措置義務）の趣旨に触れる
  - 「匿名の」IDというべきではない
- 第三者cookie（スマホアプリでは現状使用できない）
  - 提供先や流出先で個人が特定されない
  - 第三者cookie発行元サイトでのみ個人と突合できる
  - ある種の匿名ID（個人情報保護法23条、20条の趣旨に触れない?）
- アプリにローカルなID（第一者cookie相当）
  - 提供先や流出先で個人が特定されない

オプトインを必要としないケース

- 黙示の同意がある
  - 利用者の自発的な入力情報送信はそれ自体が同意によるもの
    - パスワード入力を伴うログイン時のユーザIDの入力を含む
    - 自発的な発声、カメラ撮影、ファイルアップロード等を含む
      - 目的外使用しない前提で
  - ウェブのブラウザが自動送信するのと等価な情報の自動送信
    - IPアドレス、ブラウザ名（UserAgent）、OSバージョン、URL等
  - アプリにローカルなID（第一者cookie相当）の使用
  - サービス実現（利用者が期待する）のために技術的必然性のある処理により結果的に生ずる情報取得
    - 目的外使用しない前提で
- オプトアウトで許容される
  - 第三者cookieのIDを用いたアドネットワークによる履歴収集
    - 当該アドネットワーク配備サイト上の履歴に限る

オプトアウト方式

- 原則的には望ましくない
  - オプトアウト手段の存在を知らない利用者の存在
    - オプトインを嫌がる理由が事業者にないならばオプトイン方式にすればよい
      - スマホのアプリの場合は利用者はインストールという手順を踏むのだから、そこでオプトインの手順が入っても事業者側は困ることではないはず
  - 不完全なオプトアウト手段しか提供できない現状
    - フラグcookieによるオプトアウトはオプトアウト設定が消えてしまう
    - 複数のサービスに対してオプトアウトして廻る必要があり現実的でない
    - これらはDo Not Trackで解決される
- オプトイン方式が現実的でなく有用性が勝る場合
  - 例
    - コンテンツ上の広告
      - ただし第三者cookieによるトラッキングに限る（グローバルIDを用いたものはオプトアウト方式では許容されない）
    - Wi-FiアクセスポイントのMACアドレスを用いた位置測位システム（MACアドレスを傍受される側の同意）
    - Google Street Viewの無差別撮影写真掲載

基準適用例（未完）

- アドレス帳の使用
  - 個別的選択オプトインが望ましい（Facebook等の例）
  - アプリによっては強制オプトインや黙示の同意でよい場合も
    - 例えば、アドレス帳編集機能が主体のアプリの場合
- 詳細な位置情報の使用
  - ウェブブラウザでは個別的選択オプトインになっている
    - 位置情報を必要とした時点でサイト単位での同意確認が出る
  - iOSではアプリ単位で包括的選択オプトインになっている
  - アプリ内容によっては個別的選択オプトインが望ましいのでは
- （コンテンツ内）アクセス（利用状況）解析
  - 第一者cookie（ローカルID）使用の場合は黙示の同意でよい
    - ただし、コンテンツ内操作履歴については分野ごとのコンセンサスが必要
  - 第三者cookie使用の場合はオプトアウト方式が必要
  - グローバルID使用は基本的に許されない（技術的に不必要）

基準適用例（未完）

- 他のIDとの連携
  - 個別的選択オプトイン（連携を許可するボタン）
  - 例：spモードにおけるOpenIDを用いたPPIDの払出し場面
- 登録済みの住所氏名カード番号等
  - 個別的選択オプトイン
- アドネットワーク外を含む閲覧利用履歴
  - 個別的選択オプトイン
    - 例：GoogleツールバーのPageRank表示機能オプションの利用

端末IDは使用しない

- そもそも不必要
  - アプリにローカルなIDを使用すれば済む場合が多い
    - 開発技術者の不勉強によるもの
- 複数アカウント登録防止用としても有効に機能しない
  - 端末IDの偽装（すり替え）を防ぐことは原理的に不可能
    - スマホではガラケーと異なりキャリアのゲートウェイを通らないため
- なりすましを許すセキュリティ脆弱性となる
  - 端末IDで利用者識別をしている場合、他人の端末IDの送信で、その人になりすまして操作できてしまう欠陥となる
    - 個人情報（履歴等のプライバシー情報）の漏洩、不正操作等の被害
    - 他人に自分向けの行動ターゲティング広告を見られる被害
- 一般のPCでは使用してこなかった歴史
  - 米国でも端末IDの使用は非難の対象

第三者cookie

- 第三者cookieによるIDがオプトアウトで許容される理由
  - 提供先や流出先で個人が特定されない
    - IMEI、UDID等のグローバルIDとは性質が異なる
  - 発行元でのみ個人特定情報との突合が可能だが、それをしない約束を条件にオプトアウト方式で許容される
    - 米国DoubleClick社集団訴訟の和解条件（2002年）
- これは特殊ケース
  - このケースに引きずられて、他のケースでもオプトアウトで許容せよと主張するのは合理性がない
- なお、スマホでは現時点ではこの機能は実現できない

議論を要する事項

- 情報元の種類による個別の判断
  - 例：カメラやマイクその他一部のセンサーの使用
    - データを加工しプライバシー性を低減して送信する場合であっても、撮影や録音をすること自体にオプトインを要するのではないか
- 分野ごとのコンセンサス形成が必要な領域
  - 例：「電子書籍」と謳われたアプリ
    - コンテンツ内のページ閲読状況まで記録して送信することは、オプトインを要するのではないか（業界で決める必要があるのでは？）
  - 例：音楽再生
    - コンテンツの購入履歴がオプトインなく利用されるのは許容されると考えられるが、再生履歴の利用はオプトインを要するのではないか

基準の現実性と課題

- 広告モジュールでの位置情報の使用
  - 広告モジュールにオプトインはあまり現実的でない
  - 国別の広告を配信するために位置情報を用いる例が散見される
    - 詳細な位置は不要で、他の手段を用いるべきでは
  - 詳細な位置情報を用いた広告配信は別格でオプトインが妥当
- 端末IDなしではアプリ間行動ターゲティングが実現不可
  - スマホアプリでの第三者cookie機能の欠如
    - アプリに他のアプリを重ねるインラインフレーム機能をOSが提供する等の解決策
      - 第三者cookieのIDによるアドネットワークと同等にオプトアウト方式で許容
- フィーチャフォン（ガラケー）の契約者ID/端末ID送信
  - キャリア各社はスマホへ全面移行中と思われる
  - 経過措置として当面黙認せざるを得ないのが現実
    - せめて包括同意をとるべきでは？（ソフトバンクモバイルは初回使用時に実施）
  - キャリアGWで付与するものについてはなりすまし抑制手段あり

その他

- 用語の誤用が散見される
  - オプトアウト方式においてオプトアウト前の状態を「オプトイン状態」と誤用（アドネットワーク事業者）
  - オプトインの取り消しのことを「オプトアウト」と誤用
- 何をオプトアウトするのか誤った説明
  - 停止するのは広告の配信なのかトラッキング（IDを用いた履歴収集）なのか（米国動向「Do Not Track」との関係）
- 利用者に理解されるためにできること
  - 用語の標準化
    - 「オプトイン」は利用者に見せる言葉ではないと思う
  - オプトアウト手段提供画面の標準化
  - オプトイン手続きの優れた事例の紹介（表彰等）